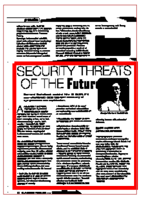
european RESELLER



N° and issue date : 41101 - 14/11/2004
Circulation : 10000
Periodicity : Quarterly
EUROPEANRESELL_41101_62_318.pdf
Web Site: http://www.europeanreseller.com

Page : 62
Size : 100 %

SECURITY THREATS OF THE Future

Gerhard Eschelbeck explains how to tackle the ever-shortening cycle between discovery of vulnerabilities and exploitation.

Qualys' Gerhard Eschelbeck

A new breed of automated, Internet-born viruses and worms has taught security managers that relying on human action alone does not work. In each case of recent damaging strikes, we've had advance warning – weeks, even months – to prepare for known vulnerabilities. Yet attackers still were able to hit hundreds of thousands of PCs and servers, crippling vital businesses and services and causing other havoc.

The uncertainty of conventional, human-led security efforts frustrates many security managers who are trying to guarantee protection. New research analysing more than 3.8 million network vulnerabilities during a recent 30-month period shows the frustration is warranted. The data were a statistically valid saınple anonymously drawn from more than six million scans made by Global 2000 organisations that were auditing network security. We learned:

- ***Half-Life:*** *the half-life of critical vulnerabilities is 21 days on external systems and 62 days on internal systems, and doubles with lowering degrees of severity.*

- ***Prevalence:*** *50% of the most prevalent and critical vulnerabilities are replaced by new vulnerabilities on an annual basis.*

- ***Persistence:*** *the lifespan of some vulnerabilities and worms is unlimited*

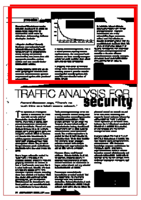
- ***Exploitation:*** *the vulnerability-to-exploit cycle is shrinking faster than the remediation cycle. 80% of worms and automated exploits are targeting the first two half-life periods of critical vulnerabilities.*

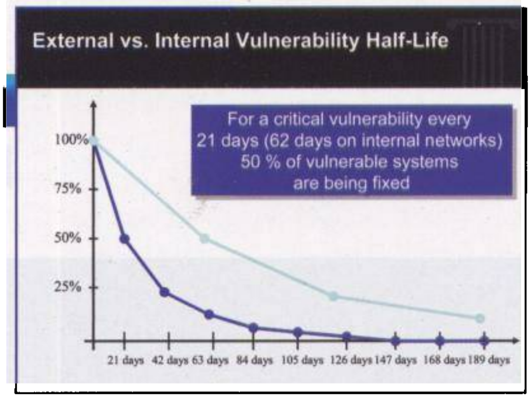
These 'laws of vulnerabilities' describe the effects of human-based security efforts, and the persistent ability of attackers to gain full control of systems – including access to highly sensitive information. Resolving issues revealed by this research requires understanding the causes and means for prevention. CIOs, chief security officers, network managers, IT managers, and security specialists should consider new trends in attack technology. Exploitation is becoming faster with the aid of new automated attack tools that require no special skills for operation. The most effective way to thwart these challenges is to supplement security efforts by humans with automated defences.

TAKING CHARGE WITH AUTOMATED DEFENCES

The implications of persistent vulnerabilities and hyper-propagation require addressing network threats in a new way. In the past, the discovery/attack lifecycle curve was one or two years from advent of discovering a vulnerability to widespread exploitation. Urgency is now rising from a shorter discovery/attack curve – SQL Slammer happened six months after discovery, Nimda was four months, Slapper was six weeks, Blaster came just three weeks after news of the vulnerability, and the Witty worm struck the day after announcement of the vulnerability. The most recent attacks happened faster than any possible human response.

N° and issue date : 41101 - 14/11/2004
Circulation : 10000
Periodicity : Quarterly
Page : 64
EUROPEANRESELL_41101_62_318.pdf
Size : 99 %
Web Site: http://www.europeanreseller.com





External vs. Internal Vulnerability Half-Life

For a critical vulnerability every 21 days (62 days on internal networks) 50 % of vulnerable systems are being fixed

Threats of the future require security managers to make an equal-force response to automation tools used by attackers. Automating defence strategies include:

- ***Regular Audits of Security Systems:*** *new automated audit solutions delivered over the web identify everything susceptible to attack, identify and prioritise vulnerabilities, and match them with appropriate remedies, such as patches and new security-device configuration settings.*

- ***Keep Antivirus Software Up-to-Date:*** *server-based solutions allow automatic scans to ensure systems are protected against older, persistent vulnerabilities.*

- ***Timely Patch Management.*** *This is a critical process requiring manual implementation, but automated audit scanners can keep security managers posted on which systems need urgent care and facilitate remediation.*

- ***Ongoing Evaluation of Security Policy.*** *Trend analysis with automated scanning solutions provides data for ensuring that security systems help meet the ever-changing nature of attack threats.*

In summary, network security attacks are increasing in number and sophistication. Research demonstrates that many vulnerabilities linger, sometimes without end. New attacks are capable of spreading faster than any possible human response effort. The timely and complete detection of security vulnerabilities with automated techniques and rapid application of remedies is the most effective preventive measure security managers can use to thwart automated attacks and preserve network security.

DETAILS

Gerhard Eschelbeck is Chief Technology Officer and VP of Engineering for Qualys, Inc, www.qualys.com